Active Perception and Defense in Cyberspace

Dr. Robert Laddaga
Program Manager
Information Innovation Office
Defense Advanced Research Projects Agency

2nd International Symposium on Resilient Cyber Systems

2014 08 21

The views, opinions, and/or findings contained in this presentation are those of the presenter and should not be interpreted as representing the official views or policies, either expressed or implied, of the Defense Advanced Research Projects Agency or the Department of Defense.

Today, Time Is Not On Our Side…

Time to detect and recover from cyber attacks

- Time to detect intrusion, repair and reconstitute systems is MONTHS
  - Operation Buckshot Yankee
  - Creech AFB
- Cost of repair and reconstitution is hundreds of millions of dollars

- Verizon's 2014 Data Breach Investigations Report notes "attackers are getting better/faster at what they do at a higher rate than defenders are improving their trade."
- Mandiant reports "In 2013, the median number of days attackers were present on a victim network before they were discovered was 229 days".
- Operation Buckshot Yankee (2008) – reportedly a 14-month effort just to contain a malware infestation *Symantec rated as "very low" threat level.* Other threats are much worse.
- 2011 malware infestation at Creech UAV base. "We keep wiping it off and it keeps coming back."

A Prerequisite for Cyber Defense

- We must treat the cyber domain as a perceptual-motor domain
- Think of human vision, medical diagnosis
- Key ideas:
  - Perception and action are deeply coupled
  - Feedback mechanisms are essential
  - Dynamic deployment and control of sensors
  - Look where the malware is acting and hiding

Coupling of Action and Perception

- Moving to change Point of View
  - Computationally inexpensive sensors can watch ‘everywhere’
    - Mostly provide a sense of state of health
    - Can indicate where additional focus of attention is useful
  - Must be able to sense, operate and deliver resources where action is occurring
  - Change in deployed sensors
- Action as diagnostic tool
  - If the repair works, you must have had the condition
  - Often fix is less expensive than test

Feedback Mechanisms Are Essential

- Feedback from interpretations to control of sensors
  - Quickly determine state of cyber health and areas of concern
  - Deploy sensors appropriate to concerns, to specific locations of concern
  - Configure sensors, fusion mechanisms, filters and aggregators
- Feedback from actions taken
  - Diagnostic results, + & -
  - Response to sensors and effectors

Dynamic Deployment and Control of Sensors

- Different sensors provide different cost/precision trade-offs
  - Deploy different sensors as situation changes
  - Tune sensor parameters to current situation
  - Dynamically tailor filtering and fusion operations
- Most engineering trade-offs are better done at execution time (when possible), in the context of the current situation

Avoid Searching Where the Light is Better

- Look where the malware is acting and hiding
  - Hosts
  - Inside applications
  - Inside OS resources
- Role of Network: Provide roots/islands of trust

"I'm searching for my keys."

© Jeffrey Callender

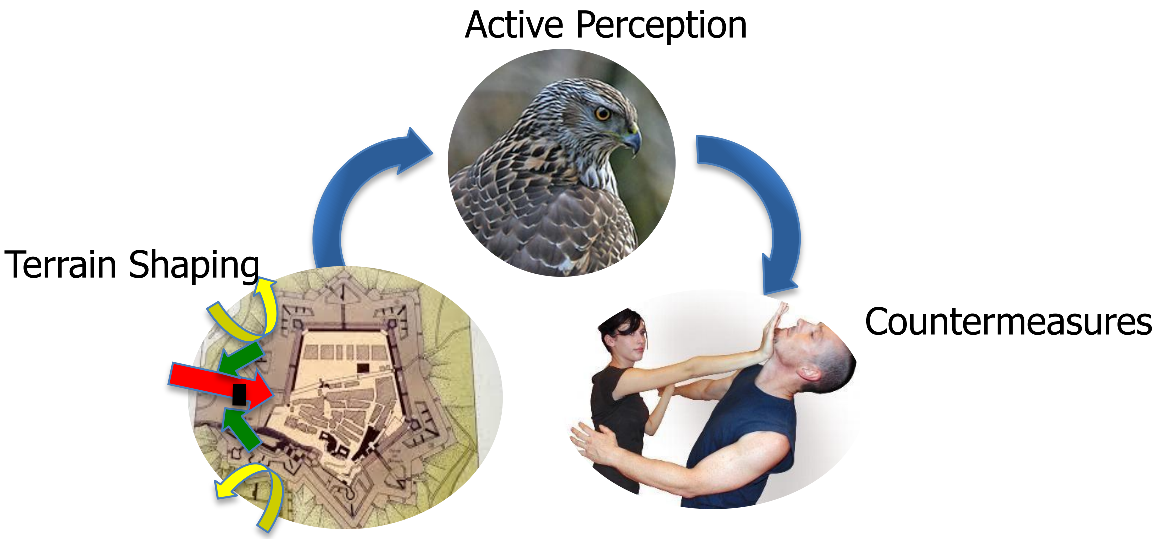
Maneuver

- Maneuver is the employment of forces in the operational area through movement in combination with fires to achieve a position of advantage in respect to the enemy. (Joint Publication 3.0: Joint Operations)
- Maneuver includes
  - Reconnaissance,
  - Surveillance,
  - Terrain shaping,
  - Counterattack, etc.
- Maneuver in cyber space
  - Highly evolved in malware/APT
    - Reconnaissance,
    - Surveillance,
    - Terrain shaping,
    - Counterattack, etc.
  - Generally Limited to ‘Moving Target Defense’ on the defense side
    - Good, but not enough…
  - Policy, legal constraints on counteraction

Defensive Maneuver in Cyberspace

Fill the holes in defensive tactics for cyberspace

- Terrain shaping – shape the engagement, canalize the attacker
- Active perception – direct sensing and fusion towards threats to the mission, apply semantically-aware sensors, focus information-gathering towards countermeasure decisions
- Active countermeasures – defeat attacks, repair damage, re-establish required resources
- ***Speed the time to detect and fix cyber attacks through autonomous cyber defense***



What Are the Holes?

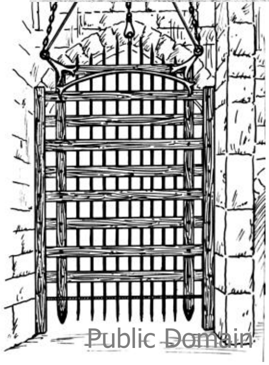
- **Terrain Shaping:** Today the terrain in cyber-space favors the attacker, not the defender.
  - Network traffic moves in a smooth mesh
  - Can't distinguish attacker movements from defender movements
- **Active Perception:** Intrusion detection is unfocused, seeing only simple surface features of network ops, plagued with blind spots and false positives, and not directed toward decision-making
- **Active Countermeasures:** Today's countermeasures are limited to blocking transmission or amputation (sacrifice an asset to try to eliminate an infection).

No Cover in Today's Cyber Terrain

D. Roddy, USGS

Fixed, unsteerable sensing

© Crown Copyright

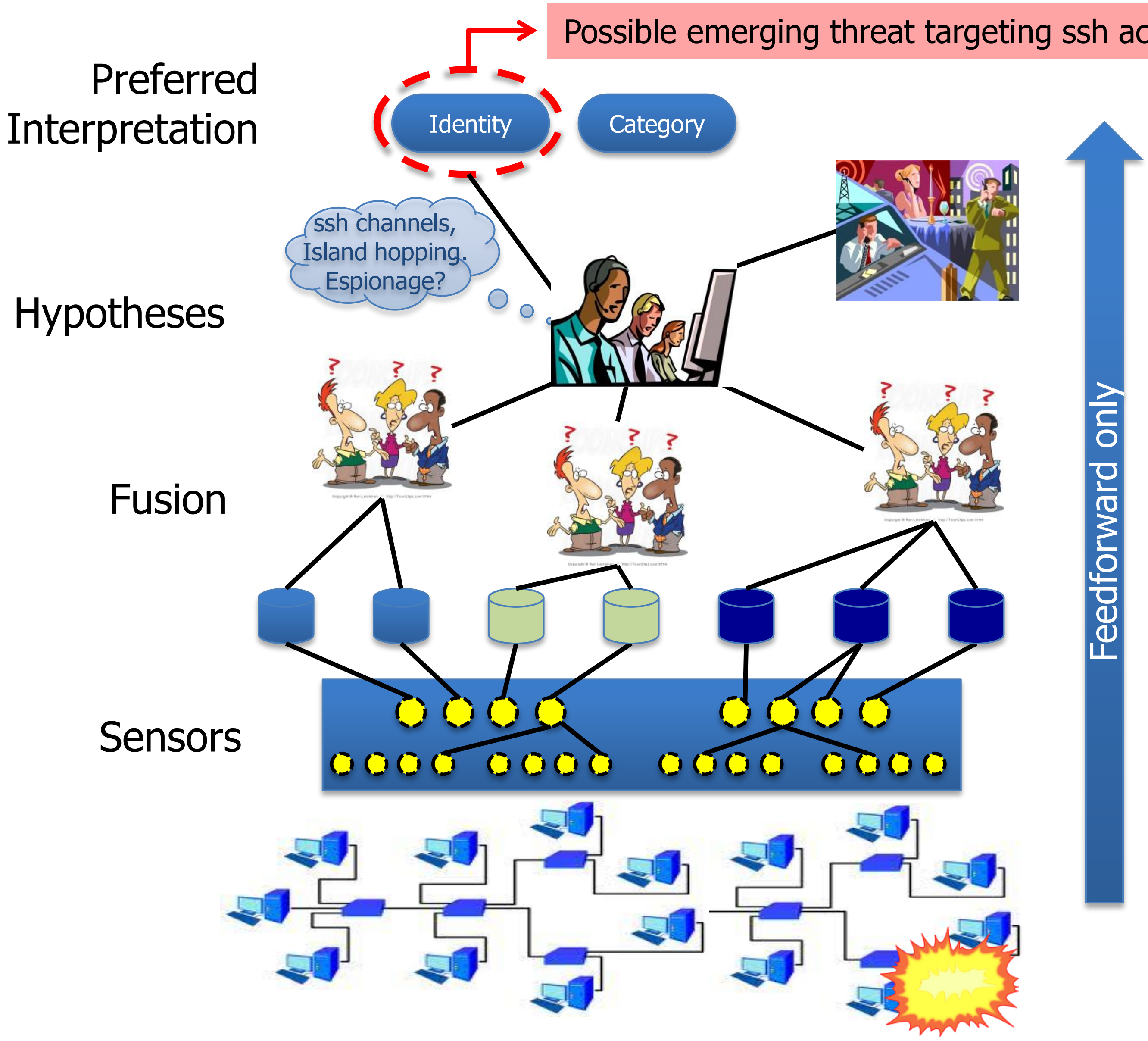


Public Domain

© National Museum of Civil War Medicine

Crude countermeasures

Sensing Today



Possible emerging threat targeting ssh across our networks.

Preferred Interpretation

Identity

Category

Hypotheses

ssh channels, Island hopping, Espionage?

Fusion

Sensors

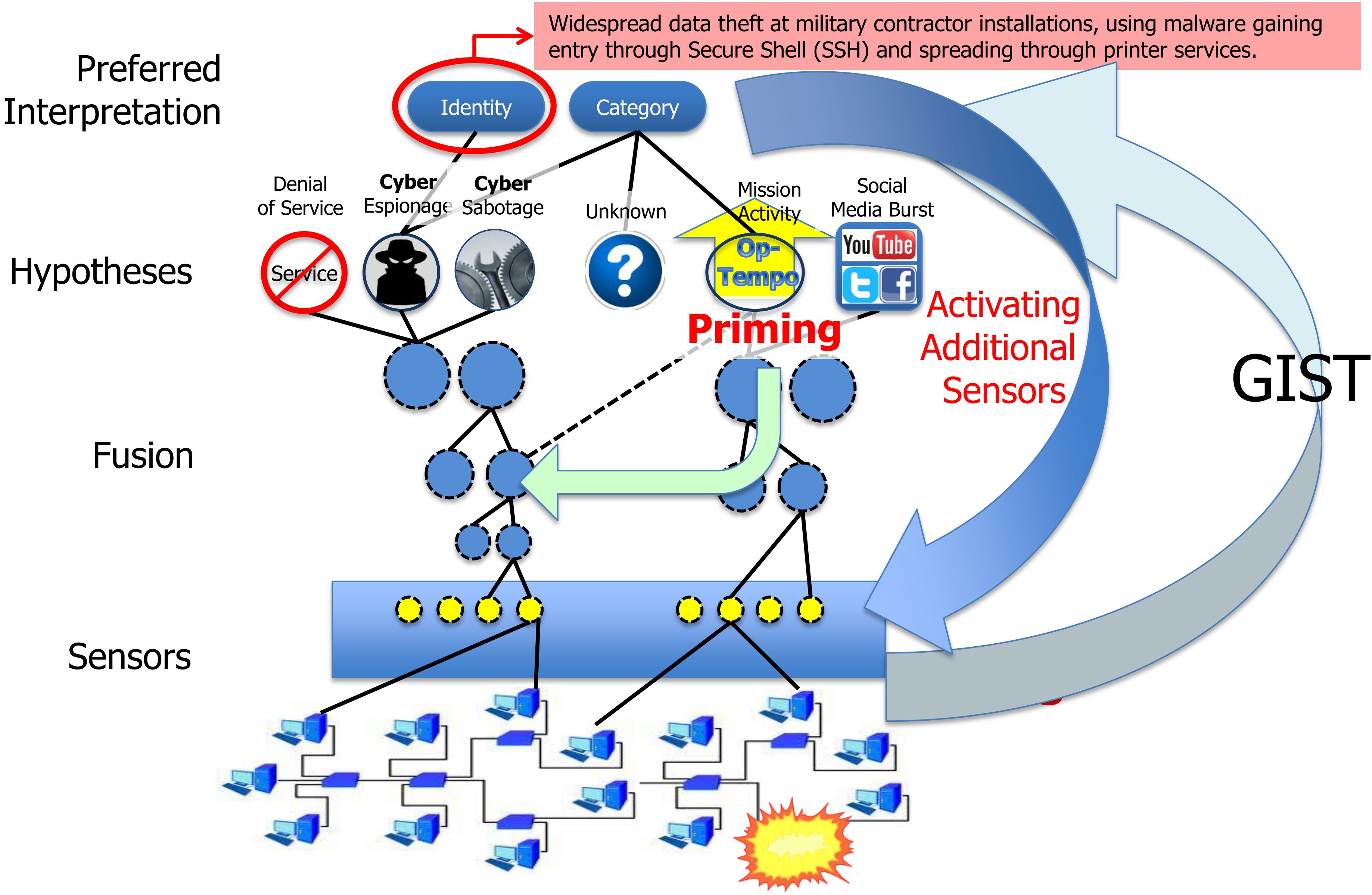
Feedforward only

- Network based
- Feed data forward
- Interpret last

Trouble is, it doesn’t work that way in natural systems.

1. Too slow, need rough understanding quickly.
2. Need top down control of sensors.

Active Perception



Widespread data theft at military contractor installations, using malware gaining entry through Secure Shell (SSH) and spreading through printer services.

Preferred Interpretation

Identity

Category

Hypotheses

Denial of Service

Service

Cyber Espionage

Cyber Sabotage

Unknown

Mission Activity

Op-Tempo

Social Media Burst

Priming

Activating Additional Sensors

GIST

Fusion

Sensors

Active Perception

© wickershamconscience 2014

- Active Perception – Feedback Driven
  - Act to perceive: controlled perceptual maneuver
  - Perceive to act: locate and destroy malware, before it can move or spread
- Active perception is a new approach to perception that utilizes biologically motivated approach
  - Not only bottom-up processing of signals
  - Also top-down expectation setting, filtering and sensor deployment
  - In predators, priming and level-jumping overcome the speed limits of neurons
  - Sensors target meaningful, actionable information
- Active monitoring, autonomous hunter killers
  - Go where the malware is
  - Destroy malware when capabilities and policy permit
  - Request permission when policy requires it
  - Reboot and re-install systems under policy and user control

© wickershamconscience 2014

Benefits of the Approach

- Reduce time to detect intrusion, repair and reconstitute systems from months to hours
- Reduce false alarms (noise reduction)
- Manage cost of the solution (sensor and countermeasure selection)
- Increase resilience by targeted application of countermeasures

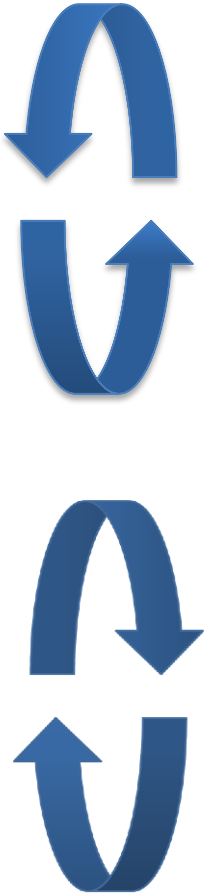
Active Perception Architecture

- Active perception (AP)
  - Domain Independent Architecture + Domain Dependent Specializations
  - Gisting: High-level sketchy situation-assessment
  - Dynamic sensor deployment, tuning, and filtering
  - Policy driven automated control of sensors + countermeasures
    - Automated cleaning, repair and limitation of spread
  - Machine learning of sensor gaps, behaviors, methods and diagnostic cues
- Terrain shaping and hardening in support of Active Perception
  - Use of protected resources to anchor AP, protect re-installing of code & data
  - Roots of trust, and islands of trusted support
  - Terrain shaping in support of AP
  - Complete efforts at hardening resources
- Formal reasoning in support of Active Perception, hardening
  - Diagnosis of data corruption and loss
  - Policy, detection, protection and response reasoning

Technical Details Active Perception

Essence of the Biologically Inspired Approach

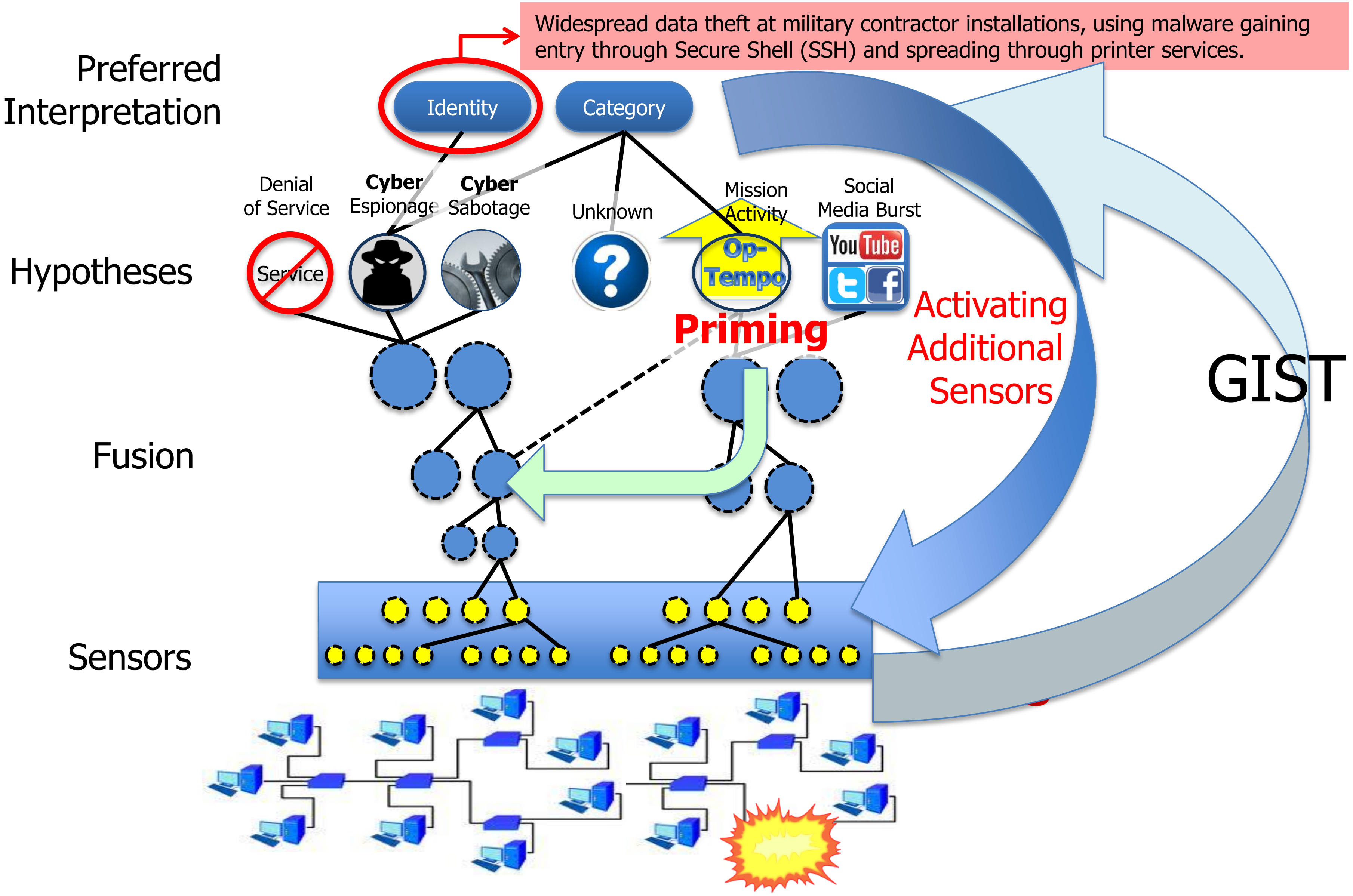
1. Get to a hypothesis set very quickly (GISTING in the vision community)
    - First step must be fast
    - Fast first step may enable 'reflex' responses while we wait for the verdict
    - This is a level-jumping step: Low level to high level
2. Adjust sensor set to help discriminate most likely hypothesis
    - Realign sensors with the perceived contexts and enable focused scrutiny
    - Hypothesis refinement stage
    - This is a level-jumping step: high to low level
3. Select small number of most likely hypotheses – hypothesis set
4. Each hypothesis establishes expectations, set up sensors for the hypothesis set
    - Limit number of hypotheses being tracked so as to improve SNR
    - This is a level-jumping step high to low level
5. Continue collecting data to improve description
    - Up and down levels without jumping
    - Use ROC curve to decide when we have enough



- *All of the above performed in the context of a desired activity (a mission) so that the value of information plays a part in the sensor choice and ROC computation.*

Active Perception

Widespread data theft at military contractor installations, using malware gaining entry through Secure Shell (SSH) and spreading through printer services.



Active Perception in Cyberspace

- Domain independent
  - Architecture
  - Control framework - requires root of trust, learning
  - Policy framework – requires policy assurance
- Domain dependent
  - Sensors
    - Targeted, dynamically deployable sensors
  - Malware Destruction/Pursuit
    - Adaptation of current malware
  - Policy contents
    - Policies to control autonomous cyber defense
  - Mixed Initiative Control
    - Supervisory control of autonomous cyber defense

Active Perception – Domain Independent

- Domain independent architecture
  - Abstract perceptual architecture that incorporates both
    - Data driven feed forward processing
    - Expectation driven feedback processing
  - Control framework
    - Based on expectation processing
    - Autonomous capability, policy constrained
    - Mixed initiative support
    - Requires root of trust hardening and terrain shaping
    - Learns new control behaviors
  - Policy framework
    - Requires policy assurance – ability to reason that policy has desirable outcomes in specified contexts

Active Perception– Domain Dependent

- Sensors
  - Broad spectrum, cheap for initial situation awareness
  - Targeted, dynamically deployable sensors for diagnosis, pursuit and refined situation awareness
- Malware Destruction/Pursuit
  - Adaptation of current malware for defensive maneuver
- Policy detail
  - Specific policies for control of autonomous defense
- Mixed Initiative Control
  - Commanders/users can assert control, seek advice
  - Autonomous systems can seek permission, advice

Sensing Process of AP

- *Gisting* activates likely candidate interpretations
- Interpretations are made of *Hierarchically structured, compositional hypotheses*
- *Hypothesis refinement:* Selecting the best candidate hypotheses, filling in supporting evidence, identifying relevant sensors
- *In-depth investigation:* Look for evidence to support/attack the hypotheses
- *Allocate computation and sensing to maximize Value of Information*
- *Fuse evidence* with models to choose the best hypotheses
- These are all applied recursively and iteratively

- *Sensor Design:* Fundamentally rethink sensor design to realize the vision of Active Perception

Active Perception Support

- Hardening and Terrain Shaping
  - Must have root of trust for AP
  - Require backup data and software be secure
  - Require secured, authenticated communication with user
  - Terrain shaping to asymmetrically advantage defender mobility
- Policy and Diagnosis Reasoning
  - Need reason to believe policies have desired outcomes in appropriate contexts
  - Need to be able to diagnose data corruption and loss

AP – Other Applications

- The active perception architecture is applicable to a wide range of sensing and signal processing tasks, including:
  - Computer vision
  - Speech recognition
  - Tipping and cueing for Intelligence, Surveillance, Reconnaissance

DARPA

www.darpa.mil